C L A I M S

1. Method for authenticating clients in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein said client comprises the steps of:

generating a header request(10),

inserting client authentication information into said header request resulting in an extended header request (20) independently of the authentication process used by said server and without server requesting authentication information,

sending said extended header request to a server (30),

and receiving information from said server if authentication has been successful (35,60).

2. Method according to claim 1, wherein said communication protocol is a HTTP-protocol.

3. Method according to claim 1, wherein said authentication information is included in the first header request for establishing a session with said server.

4. Method according to claim 1, wherein said authentication information comprises the client certificate containing client's name and client public key, and a digital signature which has been generated over a hash value of the header request including client certificate using Client private key.

5. Method according to claim 1, wherein said authentication information is automatically inserted into said header request by the Client's browser.

6. Method according to claim 5, wherein said client browser receives said authentication information from a smart card (10) via a smart card reader.

7. Method according to claim 1, wherein said authentication information is automatically inserted into said header request by a client signature component (20) which receives said authentication information from a smart card (10) via a smart card reader.

8. Method for authenticating clients (1a, 1b) in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein a system (22) establishes communication between said client (1a, 1b) and said server (3), wherein said system(22) comprises the steps of:

receiving a header request from said client(1a,1b),

inserting authentication information into said header request resulting in an extended header request(20) independently of the authentication process used by said server and without server requesting authentication information,

sending said extended header request to a server (3), and

receiving information from said server (3), if the authentication has been successful.

9. Method according to claim 8, wherein said system (20) can be a proxy server, a gateway, or a tunnel.

10. Method according to claim 8, wherein said communication protocol is the HTTP-protocol, and said authentication information is automatically inserted into said HTTP-request header by said an insertion component (20) which receives said authentication information from a signature component (24).

11. Method according to claim 8, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the whole header request including client certificate using Client's private key.

12. Method for authenticating clients in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein at said server side said method comprises the steps of:

receiving a client header request containing authentication information,

validating said authentication information contained in said header request by said server authentication component, and

providing information to said client, if the authentication has been successful.

13. Method according to claim 12, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the whole header request content using Client's private key.

14. Method according to claim 12, wherein said communication protocol is the HTTP-protocol, and said authentication component performs the steps of:
accessing said public key contained in the client certificate,
decrypting said digital signature contained in the HTTP-request header with said public key resulting in a hash value,
applying the same hash algorithm as used by said client to said HTTP-request header, and
considering authentication as successful, if both hash values match.

15. Server System (3) for authenticating clients (1) in a client-service environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein said client (1) provides authentication information in the header request to said server system, wherein said server system (3) comprising:

an authentication component (4) with the functionality to read said authentication information contained in the incoming client header request, and to validate said authentication information without having requested said authentication information from said client.

16. Client System (1) to be authenticated by a server system in client-server environment, wherein said client-server

environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein said client system comprising:

a browser (2), and

a component for inserting client authentication information into said header request independently of the authentication process used by said server and without server requesting authentication information.

17. Client System according to claim 16, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the hash value of the header request content using Client's private key.

18. Client System according to claim 16, further comprising
a smart card reader (10), and
a smart card (10) with a security module containing client's private key and a client certificate containing client name and private key, wherein said smart card provides said certificate together with a digital signature to said inserting component, wherein said digital signature is the result of an encryption of a hash value of said header request containing said certificate information by means of said private key.

19. Proxy Server system (22) for providing client authentication information to a server system (3), wherein said proxy server system (22) has a communication connection with a client system (1a, 1b) and a server system (3), wherein said communication protocol used between said systems allows

extensions of the header request of said header request without violating said communication protocol, wherein said proxy server system (22) comprising:

a proxy insertion component (20) for inserting the client certificate and digital signature into the header request received from said client independently of the authentication process used by said server and without server requesting authentication information, and

a signature component (24) for creating a digital signature and for providing it together with said client certificate to said proxy insertion component (20).

20. Computer program product stored in the internal memory of a digital computer, containing parts of software code to execute the method in accordance with claim 1-14 if the product is run on the computer.